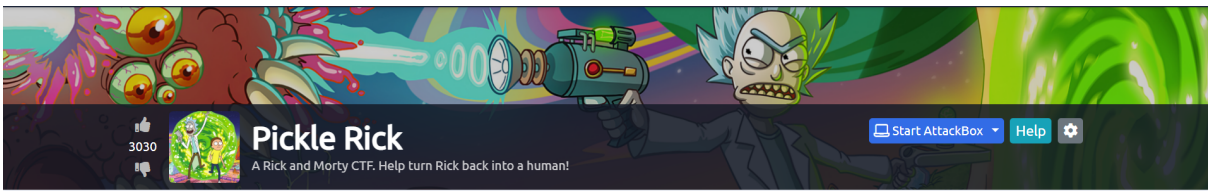


Pickle Rick

Writeup

Tryhackme

05/05/2022

En esta máquina tendremos que encontrar los tres ingredientes necesarios para que Rick pueda crear la poción para volver a convertirse en pepinillo.

Primero escaneamos la ip con NMAP y vemos los servicios con puertos abiertos, en este caso se encuentra el puerto 22 (SSH) y el puerto 80 (HTTP).

```
└─$ nmap -A -p- -T4 10.10.26.39
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-05 14:27 EDT
Nmap scan report for 10.10.26.39
Host is up (0.057s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 51:9a:20:1f:c6:44:b1:3b:79:4b:98:2b:17:64:d5:4a (RSA)
|   256 9e:fb:b9:cb:8c:82:aa:0b:63:3a:e8:38:05:03:d6:30 (ECDSA)
|_  256 0a:14:a8:7b:14:f3:bf:0a:47:d1:9f:72:a6:ef:90:c8 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Rick is sup4r cool
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.45 seconds
```

Accedemos a la web del puerto 80 y vemos que nos encontramos.

Help Morty!

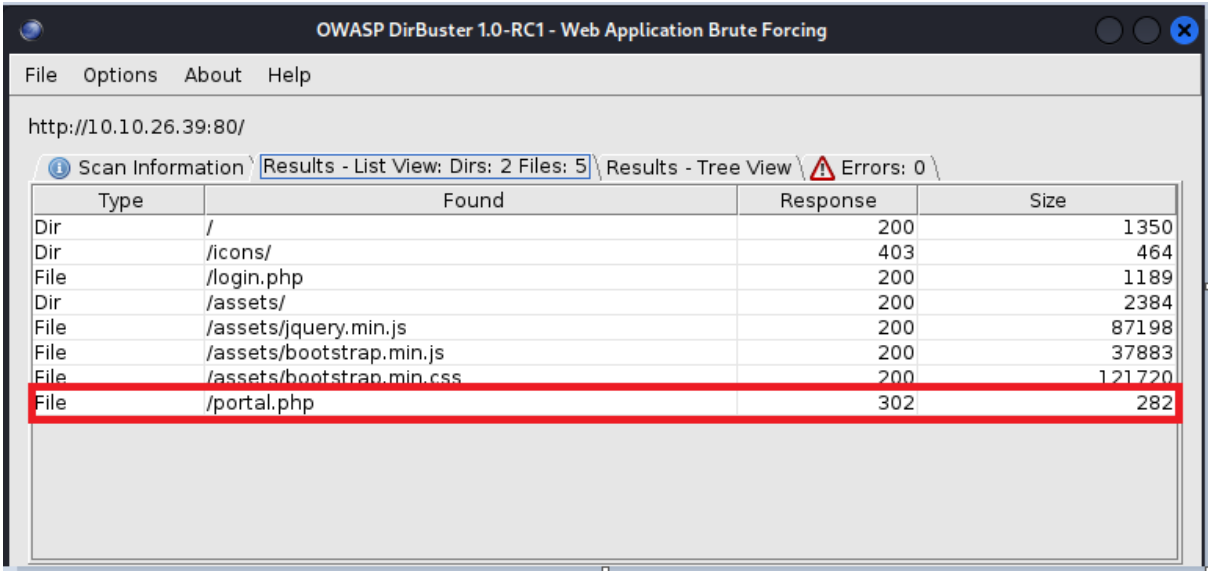
Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

Nos encontramos con esta web sin mucha información, pero podemos ver el código fuente de la web a ver que podemos encontrar.

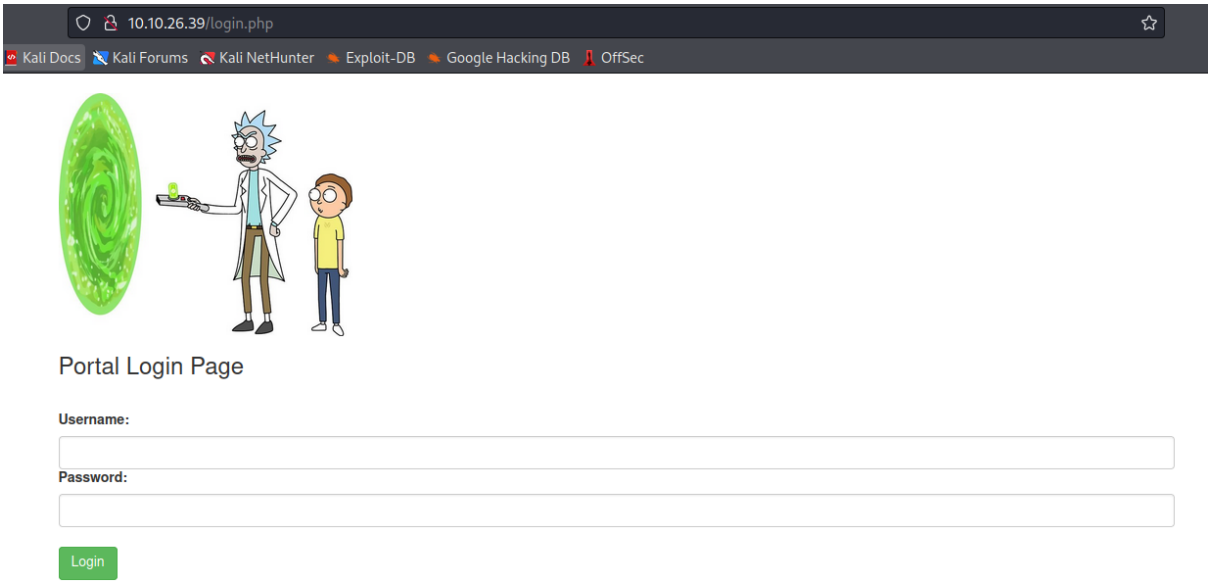
```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
  <style>
  .jumbotron {
    background-image: url("assets/rickandmorty.jpeg");
    background-size: cover;
    height: 340px;
  }
  </style>
</head>
<body>

  <div class="container">
    <div class="jumbotron"></div>
    <h1>Help Morty!</h1></br>
    <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></br>
    <p>I need you to <b>*BURRRP*</b>...Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is,
    I have no idea what the <b>*BURRRRRRRR*</b>, password was! Help Morty, Help!</p></br>
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRul3s

  -->

</body>
</html>
```

Observamos que tiene en oculto la web un usuario.
Ahora ya tenemos un usuario pero no dónde acceder, por ello vamos a hacer un DIRBUSTER a ver si encontramos algún portal de login.

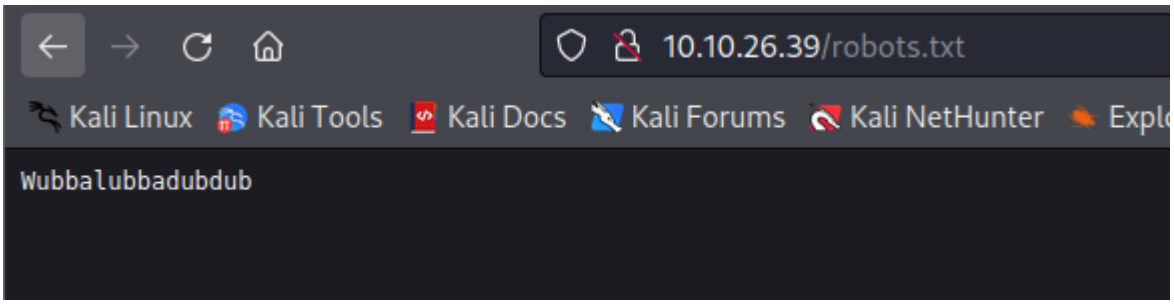


Type	Found	Response	Size
Dir	/	200	1350
Dir	/icons/	403	464
File	/login.php	200	1189
Dir	/assets/	200	2384
File	/assets/jquery.min.js	200	87198
File	/assets/bootstrap.min.js	200	37883
File	/assets/bootstrap.min.css	200	121720
File	/portal.php	302	282

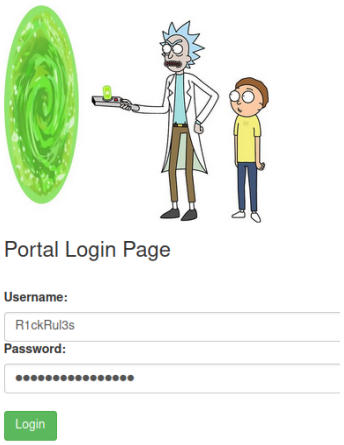
Hemos encontrado un archivo php (portal.php) que tiene pinta de ser un login.

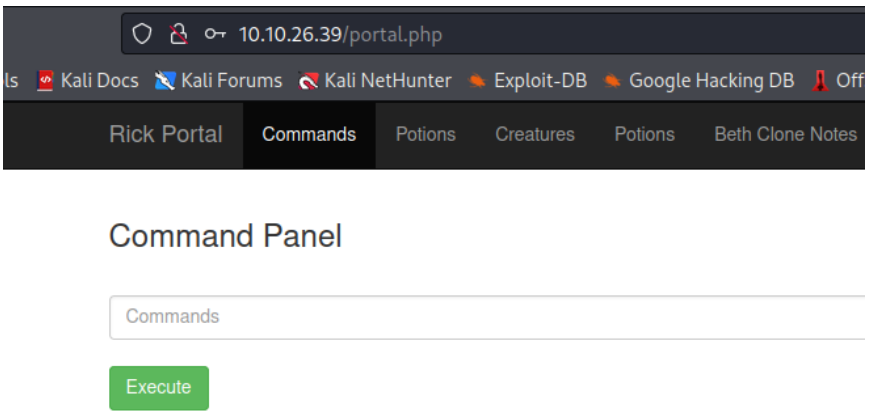


Accedemos y encontramos un login, pero claro solo tenemos el usuario, vamos a intentar buscar en algún lado la posible contraseña, vamos a ver el archivo robots.txt.

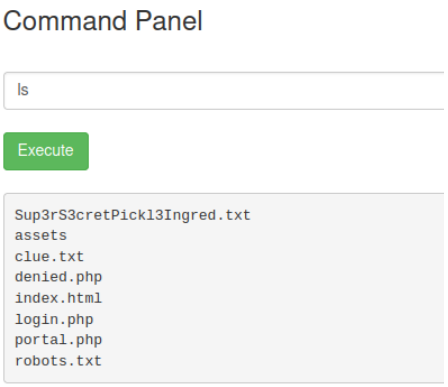


Parece ser que puede ser la contraseña, vamos a comprobarlo.

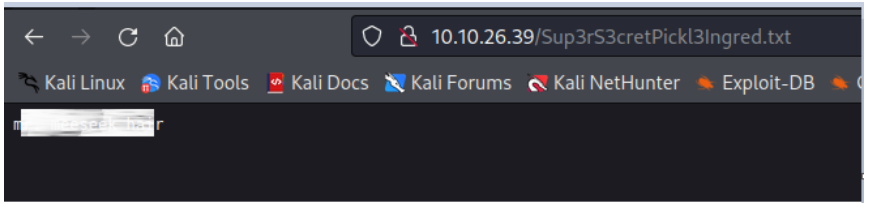




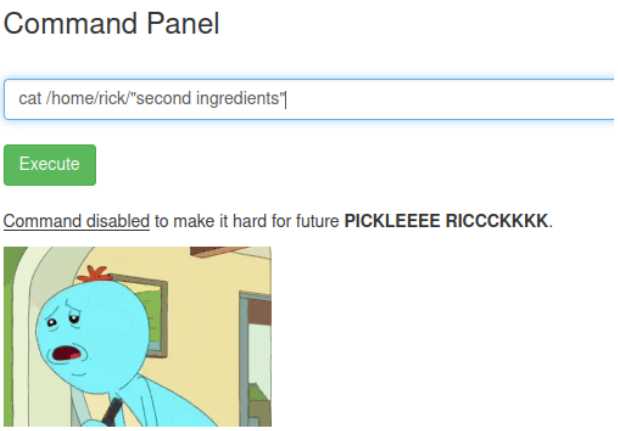
Hemos conseguido acceder, se puede observar que tiene una especie de panel para introducir comandos dentro de la máquina.



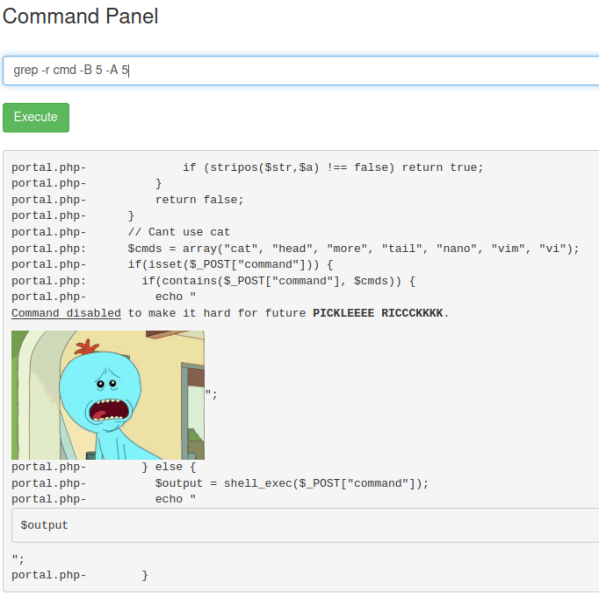
Hacemos un simple comando ls para listar los archivos y encontramos un archivo txt que puede ser el primer ingrediente, así que vamos a intentar ver su contenido, también podemos ver que nos encontramos en el directorio /var/www/html ya que estan los archivos de la web, por lo tanto accedemos desde la url para ver el posible ingrediente.



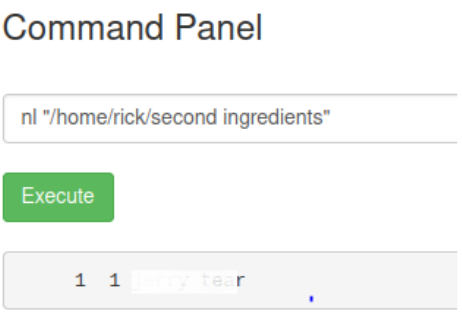
Sí, hemos encontrado el primer ingrediente, para el siguiente veamos el directorio de algún usuario que encontremos. En el directorio del usuario Rick encontramos un archivo txt con el nombre de second ingredient, vamos a intentar ver el contenido.



Si intentamos ver el contenido no nos deja, por lo visto el comando cat no está permitido, veamos qué comandos están también bloqueados.



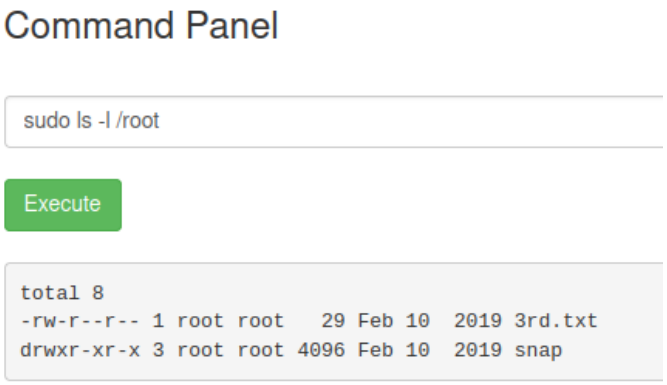
Ahora sabemos que comandos no podemos ejecutar, por lo tanto vamos a buscar otros comandos para listar que no estén entre los anteriormente puestos.



Con nl podemos ver el contenido del archivo y ver el segundo ingrediente.

Por último intentemos ver el contenido de la carpeta root a ver si podemos encontrar el último ingrediente, para ello vamos a ver los permisos de los que disponemos.

Vemos que somos el usuario www-data y que tenemos todos los permisos por lo tanto podemos ver el contenido de la carpeta root.



Se encuentra un archivo txt con el último ingrediente, lo listamos con el anterior comando y tendríamos la prueba completada.

Gracias por ver este writeup.